

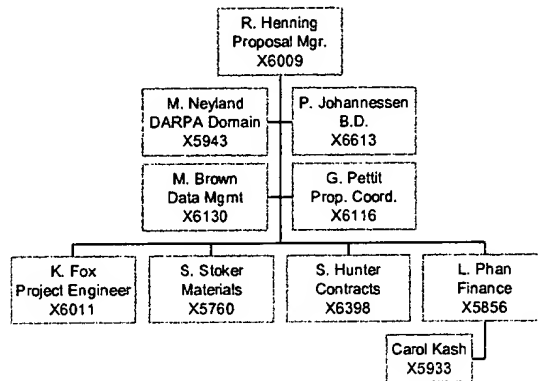
NVT2- Proposal Kickoff

Technical & Cost

25 September 1998

NVT2, *

Proposal Structure



NVT2 - Background



Program Name: NVT-2 (Information Assurance for the Next Generation
Information Infrastructure BAA)

Customer: DARPA/ISO/Information Infrastructure/Information Assurance

Program Manager: O. Sami Saydjari (on assignment from NSA)

Program Value: \$1M, 18 month schedule, CP/LOE
3 1-month options for ACTD Support
(\$11M confirmed in pool, expect at least 8 awards)
Usually MIPR to RL for execution

Schedule: 10 September- Announcement
30 October - proposal submittal
15 December - initial contractor selections expected
28 February - contract award

Scope of Work



- Building off of the NVT Study:
 - Augment NVT prototype with new functionality:
 - temporal based reasoning
 - vulnerability thresholds
 - reasoning with uncertainty or incomplete data
 - Incorporate vulnerability databases:
 - SEI/CERT Database
 - STAT from GCSD
 - Possibly later version of RAM

NVT Concept



System
Description

- Input once and normalize for all tools
- Negotiate to fill in gaps
- Create understandable report

Current NVT

Fix these
problems

DARPA Enhancements

COTS
Risk
Tool -
ANSSR

COTS
Risk
Tool -
RAM

COTS
Risk
Tool -
ISS

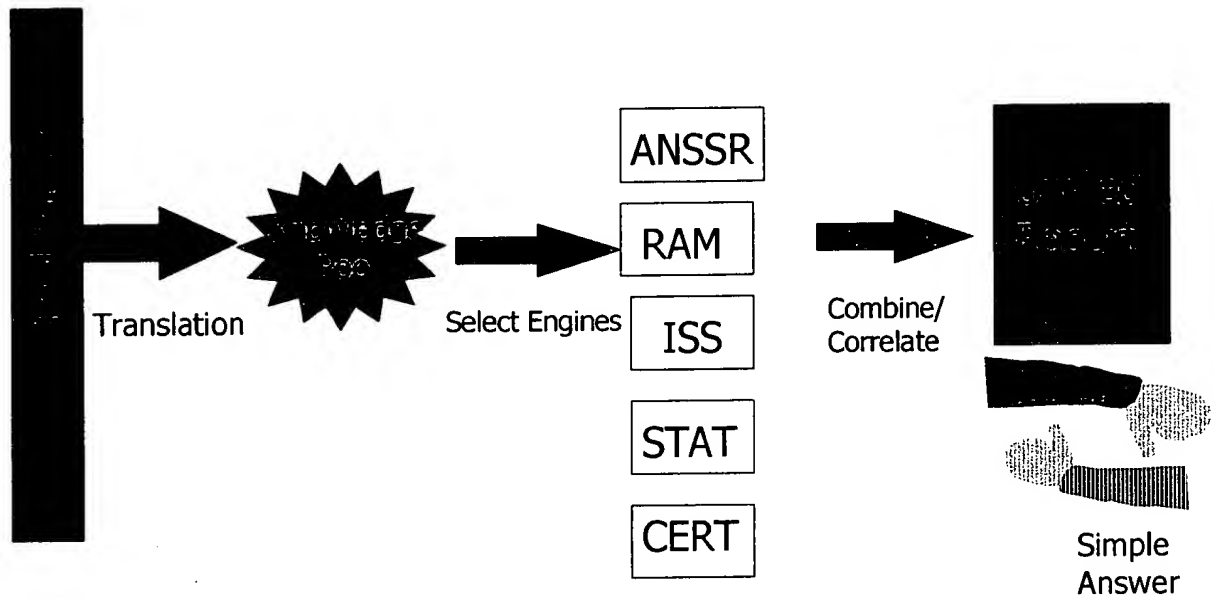
COTS
Risk
Tool -
[REDACTED]

COTS
Risk
Tool -
[REDACTED]

Deliverables: Technical reports/research papers
POC 6 month incremental prototypes to completion.

NVT Architecture

HARRIS
Electronic Systems



Cost Approach



- Scientific and Technical Merit
- Potential contribution and relevance to DARPA Mission
- Capabilities & related experience
- Plans and capability to accomplish technology transition
- Best Value

Cost Strategy:

Technically superior, can't live without it, priced in line with historical value of previous awards (\$1M -1.2M)

Best resource mix over life of program:

Travel
Materials
Labor

Proposal Schedule



ID	Task Name	Sep 20, '98							Sep 27, '98							Oct 4, '98							Oct 11, '98							Oct 18, '98							Oct 25, '98						
		M	T	W	T	F	S		M	T	W	T	F	S		M	T	W	T	F	S		M	T	W	T	F	S		M	T	W	T	F	S		M	T	W	T	F	S	
1	Bid/No Bid Decision	■																																									
2	Proposal Prep Schedule		■																																								
3	Proposal Budget Allocation		■																																								
4	Proposal Kickoff				■																																						
5	Cost Vol. Kickoff				■																																						
6	Annotated Outline Review												■																														
7	Draft Text & Art Preparation																																										
8	Materials List Due																																										
9	Consulting Decision Due																																										
10	Cost Inputs Due																																										
11	Engineering Review																																										
12	Red Team Review																																										
13	Pre-Pricing																																										
14	Cost Red Team																																										
15	Price Clearance Review																																										
16	Final Cost Adjustments																																										
17	Last Author Inputs																																										
18	Prop Center Production - F/P																																										
19	Bench Reviews																																										
20	Print/Assemble																																										
21	Bookcheck/Box																																										
22	Ship																																										
23	Due to Customer																																										
24																																											
25																																											

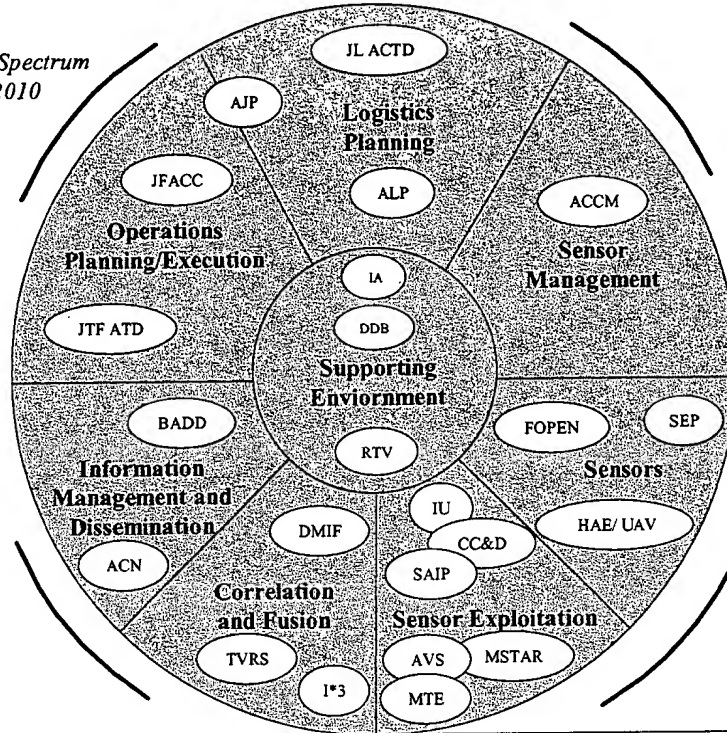
DARPA ISO - Battlefield

Awareness

HARRIS
Electronic Systems

Goal:
Dominate the Conflict Spectrum
JCS Joint Vision 2010

Enabled By:
Comprehensive
Battlespace Awareness



Leverage Network Vulnerability Tool (NVT)

- Sizeable advantage/funded headstart
 - RL study (RL is DARPA's agent for this technology)
 - Quarterly review in July -- with interested organizations
- DARPA Feedback
 - "You have enough ideas here to fund a major DARPA program by yourself"
- Only non-DARPA sponsored attendee at DARPA workshop
 - Feedback side session with Sami
- Competing Program: IOPS for ESC -- unawarded
- Possibly include a HPKB consultant for correctness
- Incorporate GCSD's STAT vulnerability database

Competitive Assessment



- Awards on merit -- no head to head competition
- Probable submitting companies
 - Boeing
 - GTE/BBN
 - SRI
 - TIS Labs @Network Associates
 - Trident Data Systems?

WIN THEMES



We have been conducting ongoing research in this area for 2 years.

NVT provides a clean, modular framework, readily expandable.

No one tool can cover everything, so why not use multiple tools to get a better answer?

With the enhancements of NVT2, the environment can be:

- a design tool for new networks*
- an assesment tool for existing networks*
- a way to prioritize problems*
- a predictive IW probability of attack tool*

New technological developments/threat models fit

Application of message understanding, data fusion, and KBMS technologies is innovative in the IA domain -- and we've been doing it!

Not a shotgun wedding.

Long term vision



- NVT becomes the standard vulnerability environment
 - Combines GOTS/COTS into unique capabilities
- CORE technology for ISO/IA
 - Before every system gets turned on,
 - Use NVT to validate risk posture
- Eventual inclusion as NGII standard environment

Proposal Assignments/Pgs.



Section	Pg Count	Author
A. Cover Page	1	Henning
B. Exec Summary	1	Henning
C. Proposal Roadmap	2	Henning
D. Cost & Fee Roll-up	1	Henning/Phan
E. Innovative Claims	1	Henning/Fox
F. Sow	20	Henning/Fox/Neyland
G. Results	1.5	Fox
H. Milestones & Schedule	1	Fox
I Technical Plan	8	Henning/Fox
J. Demo & Integration	1.5	Henning
K. Relevant Capabilities	5	Neyland
L. Management App.	5	Neyland
M. GFE/GFI	.5	Hunter
N. Proprietary Claims	.5	Hunter

Risks/Mitigation



Risk	Probability	Mitigation Strategy
NVT Prototype fails to meet expectation	Low	Manage expectation through prototype replan (in progress)
Unable to transfer hardware from NVT 1	Moderate	State in assumptions, add to materials pool (<\$30K)
Using tool on a "real" ISO program	Low	Use positions on DDB & AVS to gain architecture knowledge

Selection Criteria



Award Criteria: Integrate existing and emerging technologies or fill the current identified gaps, and be able to accommodate new/emerging technologies.

Identified 6 Technology areas:

- | | |
|------------------------------------|-----------------------------|
| 1. Advanced Boundary Controllers | 4. Malicious Code Detection |
| 2. Monitoring and Threat Detection | 5. Risk Management/DSS |
| 3. Vulnerability Assessment | 6. Response and Recovery |

Key: Relevance to other programs in ISO:

JFACC	AIM	AICE	DMIF
ALP	GENOA	AVS	
JTF-ATD	BADD	DDB	

Integration of results from DARPA/NSA

NOTE: NSA CRADA for NVT pending

CDRL List



- Monthly cost and status
- Major build reports
- Lessons learned from demo tasks
- Final report
- Draft & final user's documentation
- Prototype system as residual

Cost Volume Data



NVT2 - CP/LOE, Study

Software - LOE, organic study

Only prior history is NVT1 (ongoing)

Analogous programs -- ART-X, ENDS, IA4DB

Hardware - Generic Windows NT PC's.

CDRLS -

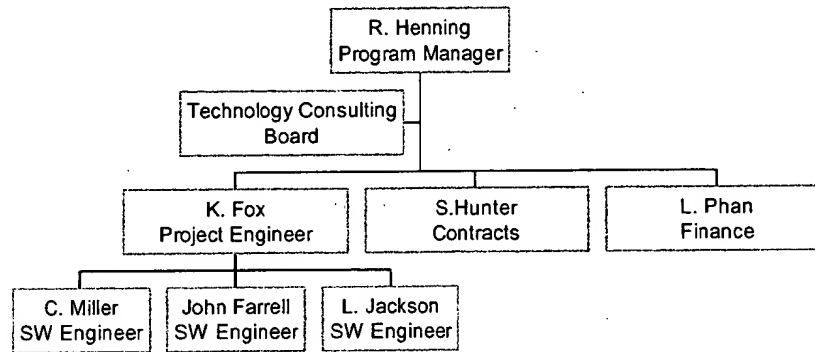
- Monthly cost and status - 20 pg.
- Major build reports 20 pg.
- Lessons learned from demo tasks 20 pg
- Final report - 75 pg.
- Draft & final user's documentation 100 pg.
- Prototype system as residual

Project Schedule



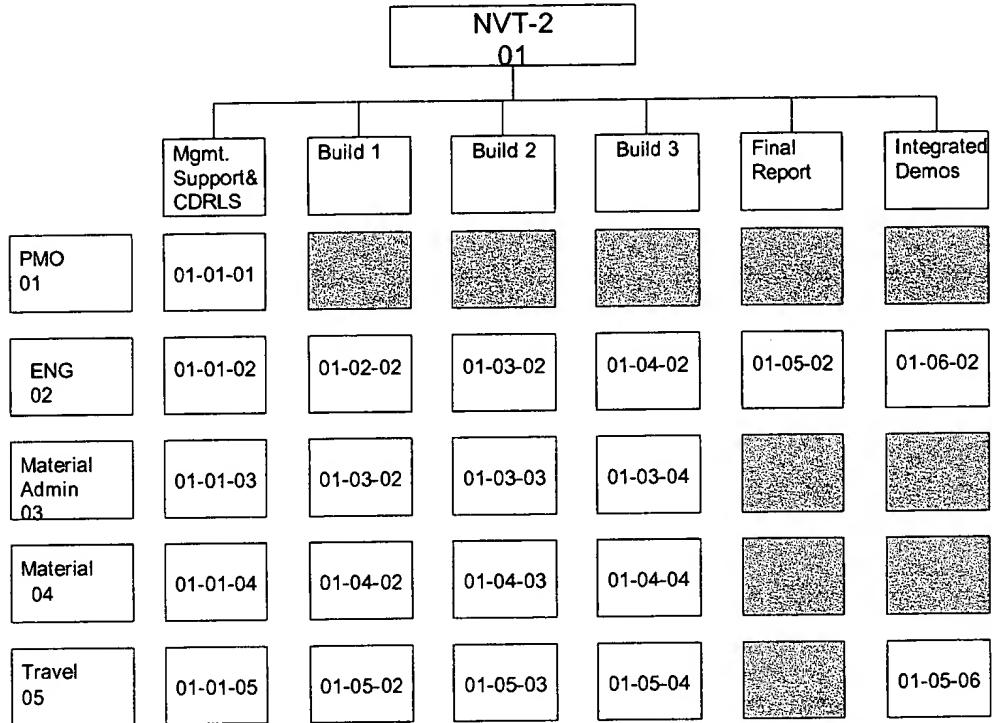
ID	Task Name	1st Quarter			2nd Quarter			3rd Quarter			4th Quarter			1st Quarter			2nd Quarter			3rd Quarter			4th Quarter			1st Quarter		
		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
1	Program Startup																											
2	Program Kickoff																											
3	Build 1																											
4	Build 2																											
5	Build 3																											
6	Monthly Cost & Status																											
25	Final Report																											
26	Quarterly Meeting																											
33	PI Meeting																											
34	PI Meeting																											
35	PI Meeting																											
36	Demo Support																											
37	Demo Support																											
38	Demo Support																											
39																												
40																												
41																												
42																												
43																												
44																												
45																												
46																												
47																												
48																												
49																												

NVT2, *



Manage as an organic study. Get our technology board to brainstorm/exchange ideas, etc.

NVT2 WBS



NVT2, *

- Assume we can keep the NVT development env.
 - If DARPA MIPRS to RL, could be ECP to NVT-1
 - Or, transfer of equipment (HW & SW Licenses)
- Means the program hits the ground running, no lead time lost
- Otherwise, impact to program of 2-3 down months
 - Waiting for HW/SW to appear after startup.
- Availability of SEI/CERT data in usable form
 - DARPA/RL funding CERT to put data in relational format.
 - Data must be available
 - Fallback -- grab the web pages
 - crude version at best.

Program Meetings



- Program Kickoff
- Quarterly Status (face to face)
 - alternating sites
- Monthly VTC/Telecons
- Every Six Months - PI meetings
 - VTC/Telconference as needed
- Demo Support
 - 30 day scheduled option
 - at completion of each functional build

Cost Targets



- Study rates
- All travel assumed to DC
- Labor hours need for:
 - PM
 - Admin
 - Engineering Support
 - Materials

Cost Bid Instructions



- Creative fictional BOEs
- Capital - none required
- Travel - To DC from Melbourne
- VTC - ??
- Materials - List due by 13 October
 - HW
 - SW packages
 - SW upgrades/maintenance

Finance Assumptions



- No capital required
 - Transfer of development hardware from NVT
- Materials to bid:
 - Extra development workstation/sw license (\$7k)
 - SW License maintenance pool (\$15K)
- Study rates (no hardware/software deliverables)
- Fee @ 10-12%